

# Reliability Standard Audit Worksheet<sup>1</sup>

## CIP-002-~~65.1a~~ — Cyber Security — BES Cyber System Categorization

*This section to be completed by the Compliance Enforcement Authority.*

**Audit ID:** Audit ID if available; or REG-NCRnnnnn-YYYYMMDD  
**Registered Entity:** Registered name of entity being audited  
**NCR Number:** NCRnnnnn  
**Compliance Enforcement Authority:** Region or NERC performing audit  
**Compliance Assessment Date(s)<sup>2</sup>:** Month DD, YYYY, to Month DD, YYYY  
**Compliance Monitoring Method:** [On-site Audit | Off-site Audit | Spot Check]  
**Names of Auditors:** Supplied by CEA

### Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		

### Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

<sup>1</sup> NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC’s and the Regional Entities’ assessment of a registered entity’s compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC’s Reliability Standards can be found on NERC’s website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity’s adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.  
~~The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity’s adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.~~

<sup>2</sup> Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

**DRAFT NERC Reliability Standard Audit Worksheet**

**Findings**

**(This section to be completed by the Compliance Enforcement Authority)**

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

**Subject Matter Experts**

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

**Registered Entity Response (Required; Insert additional rows if needed):**

SME Name	Title	Organization	Requirement(s)

DRAFT

**R1 Supporting Evidence and Documentation**

- R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [*Violation Risk Factor: High*][*Time Horizon: Operations Planning*]
- i. Control Centers and backup Control Centers;
  - ii. Transmission stations and substations;
  - iii. Generation resources;
  - iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
  - v. ~~Special Protection Systems~~ Remedial Action Schemes that support the reliable operation of the Bulk Electric System; and
  - vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above\*.
- 1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;
- 1.2.** Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
- 1.3.** Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).
- M1.** Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

\* See the full text of CIP-002-~~65-1a~~ for this reference.

**Registered Entity Response (Required):**

**Question 1:** Do you share compliance responsibility for this Requirement with another Responsible Entity?

Yes  No

For example, is any BES Cyber System located at a shared facility?

If “Yes,” list the following for each asset for which compliance responsibility is shared:

1. Asset name or designation.
2. Formal agreement or other document describing the shared compliance responsibility, if any.
3. Other information regarding the shared compliance responsibility ~~which that~~ may be useful to the audit team in determining the appropriate audit scope and approach for the asset.

Note: A separate spreadsheet or other document may be used to provide all or part of this information. If so, provide the document reference below.

**Registered Entity Response (Required):**

**Compliance Narrative:**

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

**DRAFT NERC Reliability Standard Audit Worksheet**

**Registered Entity Evidence (Required):**

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

**Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):**


**Compliance Assessment Approach Specific to CIP-002-65.1a, R1**

*This section to be completed by the Compliance Enforcement Authority*

	Verify the Responsible Entity has a process to identify each high impact BES Cyber System, each medium impact BES Cyber System, and each asset that contains a low impact BES Cyber System.
	Verify the above process considers all of the following: <ul style="list-style-type: none"> <li>i. Control Centers and backup Control Centers;</li> <li>ii. Transmission stations and substations;</li> <li>iii. Generation resources;</li> <li>iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;</li> <li>v. <del>Special Protection Systems</del> <u>Remedial Action Schemes</u> that support the reliable operation of the Bulk Electric System; and</li> <li>vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 of the Standard.</li> </ul>
	Verify the Responsible Entity has identified each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.
	Verify the Responsible Entity has identified each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset.
	Verify the Responsible Entity has identified each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any.

**Auditor Notes:**

DRAFT

**R2 Supporting Evidence and Documentation**

- R2.** The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
- 2.1** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and
  - 2.2** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.
- M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

**Registered Entity Response:**

**Compliance Narrative:**

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

**Registered Entity Evidence (Required):**

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

**Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):**


**Compliance Assessment Approach Specific to CIP-002-~~65.1a~~, R2**

***This section to be completed by the Compliance Enforcement Authority***

	Verify the reviews of the identifications in Requirement R1 have occurred at least once every 15 calendar months.
	Verify the approvals by the CIP Senior Manager or delegate of the identifications in Requirement R1 have occurred at least once every 15 calendar months.

**Auditor Notes:**

\_\_\_\_\_

DRAFT



**Additional Information:**

**Reliability Standard**

The full text of CIP-002-~~65.1a~~ may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Standards”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

**Sampling Methodology**

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

**Regulatory Language**

FERC Order No. 706

FERC Order No. 791

FERC Letter Order dated December 27, 2016, Docket No. RD17-2-000

---

**CIP-002-~~65.1a~~ - Attachment 1**

**Impact Rating Criteria**

*The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.*

**1. High Impact Rating (H)**

Each BES Cyber System used by and located at any of the following:

- 1.1.** Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
- 1.2.** Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
- 1.3.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
- 1.4** Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

**2. Medium Impact Rating (M)**

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

- 2.1.** Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
- 2.2.** Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

- 2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
- 2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- 2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

- 2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
- 2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.
- 2.9. Each ~~Special Protection System (SPS)~~, Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.
- 2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing

**DRAFT NERC Reliability Standard Audit Worksheet**

undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

**2.11.** Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

~~**2.12.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.~~

**2.12.** Control Centers or backup Control Centers, not included in High Impact Rating (H) above, that monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

<u>Voltage Value of a Line</u>	<u>Weight Value per Line</u>
<u>less than 100 kV (not applicable)</u>	<u>(not applicable)</u>
<u>100 kV to 199 kV</u>	<u>250</u>
<u>200 kV to 299 kV</u>	<u>700</u>
<u>300 kV to 499 kV</u>	<u>1300</u>
<u>500 kV and above</u>	<u>0</u>

**2.13.** Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

**3. Low Impact Rating (L)**

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

**3.1.** Control Centers and backup Control Centers.

**3.2.** Transmission stations and substations.

- 3.3.** Generation resources.
  - 3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
  - 3.5.** ~~Special Protection Systems~~ Remedial Action Schemes that support the reliable operation of the Bulk Electric System.
  - 3.6.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
- 

DRAFT

**DRAFT NERC Reliability Standard Audit Worksheet**

**Revision History for RSAW**

Version	Date	Reviewers	Revision Description
DRAFT1v0	09/19/2017 <del>4</del>	RSAWTF	New document based on CIP-002-5.1a RSAW
<u>DRAFT1v1</u>	<u>10/02/2017</u>	<u>RSAWTF</u>	<u>Changed version from -6a to -6.</u> <u>Changed version date to 10/2/2017.</u> <u>Grammatical change to item 3 of Question 1.</u> <u>Changed "Additional Information," "Reliability Standard" to match NERC web site.</u> <u>Corrected revision date of DRAFT1v0.</u>

DRAFT